Information Technology Services

WSU Tiered Administration Architecture Standard

Author(s): Matthew Kunkel & Keela Ruppenthall

Date: May 19, 2015

Version: 1.0

WASHINGTON STATE UNIVERSITY

Revision History

Version **No.**	Date	Description	Author
1.0	5/19/2016	Initial Release	Keela Ruppenthall

1. Introduction

This standard contains the Washington State University (WSU) Information Technology Tiered Administration Architecture. WSU has a responsibility to implement strategies and mitigations that limit the impact of IT intrusions into WSU information systems. Specific processes and standards are necessary for asset classification, protection, detection, response, and recovery, which are essential components to proactively establishing a more resilient defense against attackers.

This standard details an architecture designed to contribute to a defense-in-depth security administration for WSU users and resources by protecting privileged credentials.

2. Purpose

The primary purpose of this standard is to establish the specific requirements of WSU's Tiered Administration Standard.

The secondary purpose of this standard is to identify the classification, access, and configuration requirements for systems and credentials that are connected to WSU's information systems.

3. Scope

This standard applies to all WSU owned or managed information systems which perform any of the following:

3.1. Are physically connected to the WSU network

3.2. Transmit and/or receive data over any portion of the WSU network infrastructure

3.3. Process, store, or transmit WSU internal or WSU confidential data

This standard also applies to all WSU users that perform any of the following:

3.4. Connect to the WSU network

3.5. Transmit and/or receive data over any portion of the WSU network infrastructure

3.6. Involved in processing, storing, or transmitting WSU internal or WSU confidential data

4. Related NIST Controls

WSU is required to comply with Federal and/or State laws and regulations related to information security, privacy and data confidentiality. This policy complies with regulations as defined by:

- FERPA
- HIPAA
- PCI DSS v3.1 – 7.1
- GLBA
- Washington State OCIO Policy 141 – Securing Information Technology Assets

This standard satisfies part or all of the following controls from NIST Special Publication 800-53 rev4:

- AC-2: Account Management
- AC-3: Access Enforcement
- AC-4: Information Flow Enforcement
- IA-4: Identifier Management
- SC-2: Application Partitioning

5. Roles

CIO

The CIO reviews and verifies that the WSU Tiered Administration Architecture Standard is consistent with applicable Federal and State laws, University policies, and that the recommended architecture provides sufficient mitigation of risk associated with system and user administration for WSU Information Systems.

CISO

The CISO reviews and verifies that the WSU Tiered Administration Architecture Standard is consistent with applicable Federal and State laws, University policies, and that the recommended architecture provides sufficient mitigation of risk associated with system and user administration for WSU Information Systems. The CISO is responsible and accountable for monitoring adherence to the standard.

Sr. ITS Leadership

Sr. ITS Leadership reviews the WSU Tiered Administration Architecture Standard to determine the implementation feasibility of the recommended strategies and mitigations. Sr. ITS Leadership is also responsible and accountable for providing implementation and operational support.

ITS Employees

ITS employees implement, operate, monitor, and otherwise adhere to the standard in the commencement of their job duties and generally within their area of responsibility.

6. Standard

WSU Information Technology Services (ITS) adheres to a Tiered Administration Architecture that segregates systems and credentials into three distinct Tiers. The architecture is designed to reduce the risks associated with credential theft in the WSU environment. This standard defines the design principles necessary for the implementation of the Tiered Administration Architecture, ultimately limiting or slowing the impact of individual system compromises.

The following design principles are required components of a comprehensive Tiered Administration Architecture:

- Asset Inventory and Classification
- System and Credential Tier Separation
- Central Systems Management Capability Tier Separation
- Local Administrator Password Management
- Local Administrator Group Management
- Segregated Privileged Identity and Access Management
- Just in Time Credentials for Privileged Access
- Pervasive, Centralized Visibility and Audit Log Collection

Implementation, Operation, and Monitoring of these design principles reduces the risks associated with credential theft. Detection, response, and recovery processes are improved by limiting the opportunity for compromised or stolen credentials to be used freely in the environment.

7. System and Credential Tier Separation

Tiers

System and credential tier separation limits the privileges, access, and exposed credentials to which an attacker has access after the successful compromise of one or more information system components.

All information system components and user accounts (information resources) will be assigned a Tier classification upon creation.

The following outline provides the model for classifying information resources into tiers:

- Tier 0 – Universal Control and Administration:
  - Information systems or user accounts that possess the capability and access necessary to influence the access and security controls (privileged access) either to other Tier 0 resources, a majority of Tier 1 resources, or universally (i.e. Active Directory domains and domain controllers, configuration management systems, etc.)
  - Administrative workstations for Tier 0 account use and access
- Tier 1 - Data:
  - Information systems whose primary purpose is the central storage, processing, or transmission of large quantities of data, i.e. servers and layer 3+ network infrastructure devices
  - Information systems or user accounts with interactive logon access to the operating system or privileged access to a minority subset of Tier 1 resources or a majority or Tier 2 resources
  - Administrative workstations for Tier 1 account use and access
- Tier 2 – Standard Users and Devices:
  - Non-privileged users, end-user workstations, and layer-2-only network infrastructure devices
  - Information systems or user accounts with privileged access to a minority subset of Tier 2 resources

In addition to tier classifications, the following standards for separations between tiers apply:

- Each information resource (group, account, servers, workstation, Active Directory object, application, etc.) will be classified as one and only one tier.
- A higher-tier system must not depend on a lower-tier system for any form of security control.
- Users with responsibilities requiring access at multiple tier classifications will have separate accounts created for each required tier.
- Information systems will be configured to only allow accounts in a specific tier to have access that would be classified within that account’s tier, e.g. no Tier 0 or Tier 1 accounts are able to log in to lower-tier systems and Tier 2 accounts are prevented from interactive login to the operating system of higher-tier information systems.
- Tier 0 and Tier 1 assets will have egress access to internet resources only by Information Security Services-controlled exception and only with a business justification where there are no alternatives that

present lower risk.

- Local system accounts are not permitted to be used as Tier 0 or Tier 1 accounts. Built-in local administrator accounts may be used as Tier 0 or Tier 1 accounts only when necessary, but must comply with all other sections of this standard.
- Tier 0 and Tier 1 accounts will only be provisioned in a separate administrative Active Directory forest. No Tier 2 resources will exist within the administrative forest. Tier 1 information systems will not be members of the separate administrative forest, except for security monitoring systems as needed and administrative workstations.

This model is intended to minimize the presence of escalation of privilege paths that would ultimately result in unauthorized access to large data sets, especially across multiple information systems.

8. Impact Classifications

In addition to the tier classifications, each Tier 1 information system will additionally be classified into an impact classification according to the table below.

Impa ct	Confidentiality	Integrity	Availability

Low	**Public Data:** Data that are of interest to the general public and for which there is no University business need or legal reason to limit access. Public data may be made available to the general public in printed or electronic format, e.g., at the WSU library, WSU Campus Directory, WSU web sites, etc. Anyone in the general public may view these data using such public sources. However, the University does not provide these data in other than the published form(s) without the consent of the appropriate data steward and/or Public Records Officer, or as required by law. Examples of public data are employee names, work addresses, and work telephone numbers.	Data or systems for which the loss of integrity could be expected to have an adverse effect on the confidentiality or availability of other low-impact data or systems[1], or otherwise have a limited adverse effect[2] on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a limited adverse effect[2] on organizational operations, organizational assets, or individuals.
Impact	**Confidentiality**	**Integrity**	**Availability**
LOW	**Non-Public Data:** All data held by the University for operational, educational, and/or other purposes which are not appropriate or available for general public use. Non-public data shall be made		

	available to authorized University employees for inquiry/download only in support of the performance of their assigned roles/duties. Non-public data may be released to individuals or groups outside of the University community only with approval from the appropriate data steward, Public Records Officer, or as required by law. Examples of non-public data include records subject to disclosure under law including University business transactions, employee records, student records, and other data so disclosable.		
High	**Confidential Data:** Data to which access is restricted for legal or other University business reasons including personal information as described in Appendix C. Examples of confidential data include a person's name together with social security number or bank account number or driver's license number, a person's WSU Network ID together with its password, certain personnel records, certain student records, etc.	Data or systems for which the loss of integrity could be expected to have an adverse effect on the confidentiality or availability of other high- impact data or systems[3], or otherwise have a serious adverse effect[4] on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a serious adverse effect[4] on organizational operations, organizational assets, or individuals.

[1] Examples of data or systems for which the loss of integrity could be expected to have an adverse effect on the confidentiality or availability of other data or systems includes, but is not limited to: DNS, IT Systems Management, Identity

Management Systems or Applications (Devices and/or Systems), Access Control Devices or Systems (Network or System-Based), and Authentication Systems.

[2] A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to a lesser extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

9. Tiered Administration Requirements

9.1. Windows Systems

9.1.1. System Center Configuration Manager (SCCM)/SCCM Client

System Center Configuration Manager enables administrators to manage the deployment and security of devices and applications across an enterprise.

WSU Tier 0 and Tier 1 Information Systems are required to be actively managed. Tier 0 and Tier 1 Information Systems are required to have an operational SCCM client for their respective tier. Any firewalls within the communication path between the information system and the central SSCM system for the respective tier will be configured to allow all communication necessary for the following required minimum capabilities: reporting on the hardware and software inventory, reporting patch status, retrieving and applying software updates, and reporting on system configuration.

WSU Central ITS will be the custodian of the central SCCM services with access delegated for departmental management of their specific resources.

Systems failing to check in to SCCM must be identified and remediated within 30 days of the first missed check in time.

9.1.2. Secure Baseline Image

A secure baseline image is a pre-configured, security hardened, and machine ready image that contains WSU's common operating systems and applications.

All WSU Tier 0 and Tier 1 High Impact Systems are required to be deployed from SCCM Management points on their corresponding tier.

MD5 Hash verified installation media will be used to create the baseline image in order to assure the integrity of transmitted information. Specially configured USB Boot Media will be used to pull image from a SCCM Management point in order to perform the initial system imaging.

Microsoft Security Compliance Manager will be used to apply a High security configuration profile to the image. Compliance will be monitored via SCCM by the Data Center Operations team and via Splunk log analysis by the Information Security Services team.

9.1.3. Local Administrator Password Solution (LAPS)/ Group Policy Object (GPO)

LAPS is a solution that helps mitigate the risk of lateral credential escalation by simplifying local administrator account password management. LAPS is solution that combines an AD Schema extension that creates confidential attributes on AD computer objects for local administrator password storage, a small program on each endpoint that resets the local administrator account password on a system according set schedule and uploads it to the confidential computer object attribute for that system, and a GPO to control the reset schedule, password complexity, password length, and password storage location. The result is randomized, unique local administrator account passwords that rotate on a set schedule to prevent lateral traversal using common local administrator account credentials.

LAPS will be deployed to all Windows systems in all tiers. The GPO enforced password resets will be configured for a 24-hour reset cycle.

9.1.4. Just in Time Credentials (JITC)

JITC is a part of WSU’s Identity and Access Management service for privileged accounts. This solution allows accounts used for privileged access to exist in an unprivileged state, with privileges only provisioned immediately prior to use and de- provisioned shortly afterwards. This reduces the impact of a compromised privileged account by rendering it largely useless for a majority of the time.

WSU Tier 0 and Tier 1 accounts, other than built-in local administrator accounts, are required to utilize JITC.

9.1.5. Monitoring Agents

All Tier 0 and Tier 1 systems are required to submit local system audit logs into the WSU central audit log collection and analysis service in real time in order to provide pervasive real-time visibility and alerting for security-relevant events.

All Tier 0, 1, and 2 systems are required to have an installed and active advanced endpoint detection and response agent from the WSU Advanced Endpoint Detection and Response Service in order to provide rapid detection, alerting, and forensics for advanced threats.

9.2. Linux

Will be covered in a future revision of the standard.

9.3. OS X

Will be covered in a future revision of the standard.

9.4. Network Devices

Will be covered in a future revision of the standard.

9.5. Administrative Workstations

To ensure that there are no systems where credentials from multiple tiers are used in a manner that exposes them to credential theft via keystroke loggers or cached credential harvesting necessitates the use of separate workstations for activities performed within each tier. Since a higher-tier system must not depend on a lower-tier system for any form of security control, higher-tier VMs will only reside on physical hosts and storage subsystems within the same tier or a higher tier. The respective requirements for user credentials and workstations are listed in the table below.

Access Level	**System Tier**	**Required Credential**	**Source Workstation**
Interactive/Privileged	Tier 0	Tier 0	Physically Separate Tier 0 workstation
Non-Interactive/Unprivileged	Tier 0	Tier 1	Tier 1 VM or Physical Machine (May host Tier 2 VMs)
Interactive/Privileged	Tier 1	Tier 1	Tier 1 VM or Physical Machine (May host Tier 2 VMs)
Non-Interactive/Unprivileged	Tier 1	Tier 2	Any Tier 1 or Tier 2 system

Interactive/ Privileged	Tier 2	Tier 2 Administrator	Tier 2 admin physical machine (May host other Tier 2 VMs) or Tier 2 admin VM on a Tier 1 Host
All Other	Tier 2	Tier 2 User	Any Tier 2 system

10. Review Cycle

This policy will be reviewed by ITS at least once annually and updated as necessary.

Appendix A: Glossary

Acronyms

Acronym	Definition
CISO / CIO	Chief Information Security Officer / Chief Information Officer
GPO	Group Policy Object
IT	Information Technology
ITS	Information Technology Services
JITC	Just In Time Credentials
LAPS	Local Administrator Password Solution
NIST	National Institute of Standards and Technology
SCCM	System Center Configuration Manager
WSU	Washington State University

Terms

Term	Definition

Defense-in-Depth	the concept of protecting a computer network with a series of defensive mechanisms such that if one mechanism fails, another will already be in place to thwart an attack
Operational Intelligence	Real-time dynamic business analytics that enables visibility of operations